## AMENDMENTS TO THE CLAIMS

**This listing of claims will replace all prior versions and listings of claims in the application:**

## LISTING OF CLAIMS:

Claim 1 (currently amended): A system for decrypting an encrypted computer program, comprising:

means for generating a first cipher key from ~~a~~ at least one first block of the encrypted computer program;

means for ~~decrypting~~ performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key;

~~means for generating a second cipher key from one of said plurality of second blocks; and~~

~~means for decrypting another of said plurality of second blocks with said second cipher key~~

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Claim 2 (currently amended): The system as set forth in claim 1,

wherein said at least one first block is not encrypted.

Claim 3 (currently amended): The system as set forth in claim 1,

wherein said plurality of second blocks are encrypted at least with said first cipher key ~~before treaded by this system~~prior to being decrypted.

Claim 4 (currently amended): The system as set forth in claim 3,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key ~~before treated by this system~~prior to being decrypted.

Claim 5 (currently amended): The system as set forth in claim 1, further comprising:

means for ~~detecting~~ determining whether ~~or not~~ the encrypted computer program is analyzed; and

means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if ~~it is detected that the encrypted computer program is analyzed~~the encrypted computer program is determined to be analyzed.

Claim 6 (currently amended): A method for decrypting an encrypted computer program, comprising the steps of:

generating a first cipher key from ~~a~~ at least one first block of the encrypted computer program;

~~decrypting~~ performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; and

~~generating a second cipher key from one of said plurality of second blocks; and~~

~~decrypting another of said plurality of second blocks with said second cipher key~~

performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Claim 7 (currently amended): The method as set forth in claim 6,

wherein said at least one first block is not encrypted.

Claim 8 (currently amended): The method as set forth in claim 6,

wherein said plurality of second blocks are encrypted at least with said first cipher key ~~before treaded by this method~~prior to being decrypted .

Claim 9 (currently amended): The method as set forth in claim 8,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key ~~before treated by this method~~prior to being decrypted.

Claim 10 (currently amended): The method as set forth in claim 6, further comprising the steps of:

~~detecting~~ determining whether ~~or not~~ the encrypted computer program is analyzed; and

decrypting a plurality of dummy blocks instead of said plurality of second blocks if ~~it is detected that the encrypted computer program is analyzed~~the encrypted computer program is determined to be analyzed.

Claim 11 (currently amended): A computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, said method comprising the steps of:

generating a first cipher key from ~~a~~ at least one first block of the encrypted computer program;

~~decrypting~~ performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; and

~~generating a second cipher key from one of said plurality of second blocks; and~~

~~decrypting another of said plurality of second blocks with said second cipher key~~

performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Claim 12 (currently amended): The computer program product as set forth in claim 11, wherein said at least one first block is not encrypted.

Claim 13 (currently amended): The computer program product as set forth in claim 11, wherein said plurality of second blocks are encrypted at least with said first cipher key ~~before treaded by this method~~prior to being decrypted.

Claim 14 (currently amended): The computer program product as set forth in claim 13, wherein at least one of said plurality of second blocks is encrypted with said second cipher key ~~before treated by this method~~prior to being decrypted.

Claim 15 (currently amended): The computer program product as set forth in claim 11, wherein said method further comprises the steps of:

~~detecting~~ determining whether ~~or not~~ the encrypted computer program is analyzed; and

decrypting a plurality of dummy blocks instead of said plurality of second blocks if ~~it is detected that the encrypted computer program is analyzed~~the encrypted computer program is determined to be analyzed.

Claim 16 (currently amended): A data structure embodied on a computer-readable medium comprising:

a non-encrypted block; and

a plurality of encrypted blocks;

wherein said plurality of encrypted blocks are encrypted with a cipher key generated from said non-encrypted block, and

wherein ~~one of said plurality of encrypted blocks is encrypted with a cipher key generated from another of said plurality of encrypted blocks~~for each of said plurality of encrypted blocks, a next block is encrypted with a cipher key which is generated from a current block.

Claim 17 (new): A system for decrypting an encrypted computer program, comprising:

means for generating cipher keys for a plurality of blocks, and

means for performing a decryption of the plurality of blocks,

wherein for each of said plurality of blocks, a cipher key is generated from a current block and a next block is decrypted with said cipher key.

Claim 18 (new): A method for decrypting an encrypted computer program, comprising a step of:

performing a decryption of a plurality of blocks,

wherein for each of said plurality of blocks, a cipher key is generated from a current block and a next block is decrypted with said cipher key.

Claim 19 (new): A computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, said method comprising a step of:

performing a decryption of a plurality of blocks,

wherein for each of said plurality of blocks, a cipher key is generated from a current block and a next block is decrypted with said cipher key.